Cisco UCS Director Upgrade Guide, Release 5.5

First Published: 2016-06-14

Last Modified: 2016-11-03

Overview of the Upgrade to Cisco UCS Director, Release 5.5

The upgrade process to Release 5.5 depends on the current version of the software that is installed on your system. For information on supported upgrade paths, see Supported Upgrade Paths to Cisco UCS Director, Release 5.5, on page 1.

If your system is running versions prior to Release 5.4, then you must first migrate to Release 5.4, and then upgrade to Release 5.5. Cisco UCS Director Release 5.4 uses a new version of Java and the CentOS operating system. Due to this, the upgrade procedure for Release 5.4 is different from previous upgrade processes. For more information on how to upgrade your system to Release 5.4, see the *Cisco UCS Director Upgrade Guide, Release 5.4*, available at:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-installation-guides-list.html

Supported Upgrade Paths to Cisco UCS Director, Release 5.5

The following are the supported upgrade paths for Cisco UCS Director, Release 5.5:

Upgrade Paths from Release 5.4(x.x) Platform

- From Release 5.4 to Release 5.5
- From Release 5.4(0.1) to Release 5.5
- From Release 5.4(0.2) to Release 5.5
- From Release 5.4(0.3) to Release 5.5

Important Upgrading Cisco UCS Director to release 5.5 from versions prior to Release 5.4 is not supported.

Supported Upgrade Paths to Cisco UCS Director, Release 5.5 (0.1)

The following are the supported upgrade paths for Cisco UCS Director, Release 5.5 (0.1):

Important Upgrading Cisco UCS Director to release 5.5(x.x) from versions prior to Release 5.4 is not supported.

Upgrade Paths from Release 5.5(x.x) Platform

From Release 5.5 to Release 5.5(0.1)

Upgrade Paths from Release 5.4(x.x) Platform

- From Release 5.4 to Release 5.5(0.1)
- From Release 5.4(0.1) to Release 5.5(0.1)
- From Release 5.4(0.2) to Release 5.5(0.1)
- From Release 5.4(0.3) to Release 5.5(0.1)
- From Release 5.4(0.4) to Release 5.5(0.1)

Upgrading a Single Node Setup to Release 5.5

Follow this procedure to upgrade from Cisco UCS Director, Release 5.4. If you need to upgrade from an earlier release, you must first upgrade to Release 5.4. For more information, see the *Cisco UCS Director Upgrade Guide, Release 5.4* available at: http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-installation-guides-list.html.

Before You Begin

- Download the Cisco UCS Director, Release 5.5 patch from http://www.cisco.com.
- Place the software in the FTP or HTTP server that you plan to use to install the upgrade.
- If NFS mount is used for application storage, disable it before you apply a patch. If you do not, the upgrade will fail.

Note We recommend that you take a snapshot of the VM before you begin the upgrade. If you do this, you do not need to back up the existing configuration database through an FTP server.

Step 1 Start your current version of Cisco UCS Director (Release 5.4).

Step 2 In the ShellAdmin, choose `Stop services` to stop all services.

Step 3 To verify that all services are stopped, choose `Display services status`.

Step 4 (Optional) If desired, you can choose `Backup database` to back up the Cisco UCS Director database. You do not need to back up the database if you took a snapshot of the VM before you started.

Step 5 To upgrade Cisco UCS Director to Release 5.5, choose `Apply patch`.

Step 6 When prompted, enter the location of the Release 5.5 patch.

ftp://*username*:*password*@*hostname*|*IP_address*/*software_location_and_name*

Step 7 Wait for the download and installation to complete.

Step 8 When prompted, choose `Start services` to start services and complete the upgrade process.

Note After you apply the upgrade patch and complete that installation, choose the Start Services option of ShellAdmin to start/restart the Cisco UCS Director services and complete the patch process. The patch process is not complete or successful until the Cisco UCS Director services have started, Cisco UCS Director is available, the login screen is displayed, and the administration can log in to Cisco UCS Director.

All Cisco UCS Director services must be started before you attempt to perform other shelladmin procedures, such as apply additional patches, take a database backup, or restore a database from a backup.

Step 9 When the upgrade is complete, choose `Show Version` in ShellAdmin to verify the current version of Cisco UCS Director.

Upgrading a Multi-Node Setup to Release 5.5

Perform these steps on the primary node and all service nodes. This procedure also upgrades the inventory database or monitoring database nodes.

Follow this procedure to upgrade from Cisco UCS Director, Release 5.4. If you need to upgrade from an earlier release, you must first upgrade to Release 5.4 and then upgrade to Release 5.5. For information on upgrading to Release 5.4, see the *Cisco UCS Director Upgrade Guide, Release 5.4* available at:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-installation-guides-list.html.

Before You Begin

- Download the Cisco UCS Director, Release 5.5 patch from http://www.cisco.com.
- Place the software in the FTP or HTTP server that you plan to use to install the upgrade.
- If NFS mount is used for application storage, disable it before you apply a patch. If you do not, the upgrade will fail.

Note We recommend that you take a snapshot of the VM before you begin the upgrade. If you do this, you do not need to back up the existing configuration database through an FTP server.

Step 1 Start the primary and service nodes for your current version of Cisco UCS Director (Release 5.4).

Step 2 In the ShellAdmin for the primary and all service nodes, choose `Stop services` to stop all services.

Step 3 To verify that all services are stopped, choose `Display services status`.

Step 4 (Optional) If desired, you can choose `Backup database` on the inventory database and monitoring database nodes to back up the Cisco UCS Director database.
You do not need to back up the database if you took a snapshot of the VM before you started.

Step 5 In the ShellAdmin for the primary node and all service nodes, choose `Apply patch` to upgrade those nodes to Release 5.5.

Step 6 When prompted, enter the location of the Release 5.5 patch.
ftp://*username*:*password*@*hostname*|*IP_address*/*software_location_and_name*

Step 7 Wait for the download and installation to complete.

Step 8 When prompted, choose `Start services` to start services on the primary node and all services nodes and complete the upgrade process.

Note After you apply the upgrade patch and complete that installation, choose the Start Services option of ShellAdmin to start/restart the Cisco UCS Director services on the primary service nodes and complete the patch process. The patch process is not complete or successful until the Cisco UCS Director services have started, Cisco UCS Director is available, the login screen is displayed, and the admin user can log in to Cisco UCS Director.

All Cisco UCS Director services must be started before you attempt to perform other ShellAdmin procedures, such as apply additional patches, take a database backup, or restore a database from a backup.

Step 9 When the upgrade is complete, choose `Show Version` in ShellAdmin to verify the current version of Cisco UCS Director.

Upgrading Bare Metal Agent to Release 5.5

Before You Begin

- Upgrade Cisco UCS Director to Release 5.5.

  If your system is running versions prior to release 5.4, then you must first migrate to Release 5.4, and then upgrade to Release 5.5. For information on upgrading to release 5.5, see the *Cisco UCS Director Release 5.5 Upgrade Guide* available at: http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-installation-guides-list.html

Step 1 Download the Bare Metal Agent, Release 5.5 patch to the existing Bare Metal Agent.

Step 2 Log in to the Bare Metal Agent console through PuTTY or another Secure Shell (SSH) client, using the default root credentials shown or the root credentials for your system.

```
Username: root
Password: pxeboot
```

Step 3 Unzip the patch.

Step 4 Navigate to the directory of the unzipped file.

```
cd ucsd_bma_patch_5_5_0_0
```

Step 5 Run **./applyPatch.sh** to apply the patch to Bare Metal Agent.

Step 6 Navigate to the `/opt/infra` directory.

Step 7 Run **./showBMAVersion.sh** to verify that you have the correct version of Bare Metal Agent.

Step 8 Log in to Cisco UCS Director, Release 5.5, and choose **Administration** > **Physical Accounts** > **Bare Metal Agents**.

Step 9 Choose the account for the Bare Metal Agent that you have upgraded.
If your system has more than one instance of Bare Metal Agent, you can identify the correct account by the IP address.

Step 10 Confirm that the Bare Metal Agent account is reachable from Cisco UCS Director and then stop and start the services for that account.

Downloading Cisco UCS Director PowerShell Agent

You download the installer for PowerShell Agent from Cisco UCS Director.

Step 1 In Cisco UCS Director, choose **Administration** > **Virtual Accounts**.

Step 2 Choose the **PowerShell Agents** tab.

Step 3 Click the **Download Installer** button.

Step 4 Review the list of installation requirements in the **Download Agent Installer** dialog box and ensure that you have them available on the target computer where you plan to install Powershell Agent.

Step 5 Click **Submit**.
The `PSASetup.exe` file is downloaded to the default download folder on the target computer.

What to Do Next

Install Cisco UCS Director PowerShell Agent on the target computer.

Installing Cisco UCS Director PowerShell Agent

Note If you do not install the new version of PowerShell Agent for Cisco UCS Director, Release 5.5, the **Execute Power Shell Task** and the **Execute Command** options on the **PowerShell Agents** tab will not work correctly.

Before You Begin

You need system administrator privileges to complete this task.

Step 1 If necessary, copy the `PSASetup.exe` that you downloaded from Cisco UCS Director to your target computer.

Step 2 Double-click the **PSASetup.exe** file.

Step 3 In the **Preparing to Install** screen, click **Next**.

Step 4 In the **Ready to install the Program** screen, click **Install**.
The **Installing Cisco PSA Service** screen displays during the installation. When the installation is complete, the **InstallShield Wizard Completed** screen displays.

Step 5 Click **Finish**.

The PowerShell Agent is installed to the `C:\Program Files (x86)\Cisco Systems\Cisco PSA Service` folder. This folder is referred to as `%AGENT_INSTALL_FOLDER%` in the remainder of the document.

Step 6 On your computer, choose **Start**, type services.msc in the text field, and press the **Enter** key.
A list of current services displays. Verify that the Cisco PSA Service is listed and is currently running.

Upgrading Cisco UCS Director REST API to Release 5.5

The following procedure assumes that you are using an Eclipse development environment. If you use a different development environment for your REST API projects, perform the appropriate steps for that environment.

Before You Begin

The currently installed version on your system should be release 5.4. For more information on upgrading to release 5.4, see the *Cisco UCS Director Release 5.4 Upgrade Guide* available at:

http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-director/products-installation-guides-list.html

Step 1 Download the Cisco UCS Director SDK Bundle, Release 5.5 from Cisco.com.

Step 2 Import the project into Eclipse.

Step 3 Execute the examples available to understand the REST API execution. The examples are located at `com.cisco.cuic.api.examples`.

Post Upgrade Requirements

Workflows created in release 5.4 without a catalog input would fail to run after upgrading to release 5.5. This is because, selecting a catalog to provision a VM using the New VM Provision task in the ISO image workflow is mandatory in release 5.5, whereas selecting a catalog was optional in release 5.4. For a workflow to run successfully in release 5.5, you must complete the following steps:

1. Create an empty or dummy catalog.

   While creating this catalog, be sure to select the **Provision new VM for ISO mounting** check box and leave the **Image** field empty. If you do select an image, then a new VM is cloned from the selected image.
2. Open the workflow containing the New VM Provision task.
3. Edit the New VM Provision task to include the catalog.

You need not create multiple catalogs for different VM provisioning workflows. You can just create one catalog, and select it for multiple workflows.

Creating a Catalog for VM Provisioning Workflows

Step 1 On the menu bar, choose **Policies** > **Catalogs**.

Step 2 Choose the **Catalog** tab.

Step 3 Click **Add (+)**.

Step 4 In the **Catalog Add** dialog box, select the **Standard** type of catalog.

Step 5 Click **Submit**.

Step 6 In the **Create Catalog** dialog box, complete the following fields:

Name	Description
Basic Information pane	
Catalog Name field	Enter a name of the catalog. **Note** Once created, a catalog name cannot be modified.
Catalog Description field	Enter a description of the catalog.
Catalog Type drop-down list	The type of catalog. It can be one of the following: • **Standard—**Used to create catalogs for VM provisioning, using images from a list of clouds. • **Advanced—**Used for publishing orchestration workflows, such as catalog items. • **Service Container—**Used for publishing application containers as catalog items. • **Bare Metal Catalog—**Used to create catalogs for bare metal server provisioning.
Catalog Icon drop-down list	Choose from a list of icons to associate this catalog with an image. This icon is seen when you are creating a service request using this catalog.
Applied to all groups check box	Check the check box to enable all groups to use this catalog. Leave it unchecked to deny its use to other groups.
Support Contact Email Addresses field	Specify the email address of the support contacts.
Selected Groups check box list	Check the check boxes for included groups that are from the **Select Items** dialog box. The checked groups use this catalog to provision new VMs.

Name	Description
Publish to end users check box	By default, this check box is checked. Uncheck this check box if you do not want this catalog to be visible to end users. If you do not uncheck this check box, then this catalog is visible to the end users of the system.
Cloud Name drop-down list	Choose the cloud with the image for VM provisioning.
Provision new VM for ISO mounting check box	Check this check box to clone a new VM from a selected image. If you do not check this check box, a blank VM is created. If you are creating this catalog to run workflows created in prior versions, then you must check this check box, and not select an image in the subsequent field.
Image field	Choose the type of image, (any existing templates such as Windows, Linux, and other files that make up the image) that you use when VMs are provisioned using this catalog. If you are creating this catalog to run workflows created in prior versions, then you must leave this field blank. If you do select an image, then a new VM is cloned from the selected image.
Provision all disks in single datastore check box	Check the check box to provision all disks in a single datastore. You can also choose to use the datastores configured for each disk in the storage policy. **Note** This option appears if the chosen template has multiple disks. This option is not supported in the RHEV KVM Connector.
Select Folder drop-down list	Choose the folder within which this catalog must be created. **Note** The drop-down list includes names of folders that are available by default. You can either select a folder that is available, or click the + icon to create a new folder. To create a new folder in the **Add New Folder** dialog box, specify a folder name, and select an icon for the folder.

Step 7 Click **Next**.

Step 8 In the **Applications Details** pane, complete the following fields:

Name	Description
Category drop-down list	Choose a VDC category.

Name	Description
Override check box	Check the check box to enable the end user to override the selected category while provisioning a VM using a service request.

Step 9 Click **Next**.

Step 10 In the **Customization** pane, retain the default values.

Step 11 Review the summary information and click **Submit**.

Step 12 On the menu bar, choose **Policies** > **Orchestration**.

Step 13 Choose the **Workflows** tab.

Step 14 From the list of workflows, select the VMware provisioning workflow, and choose **Execute Now**.

Step 15 In the **Executing Workflow** dialog box, choose the recently created catalog in the **Select Catalog** drop-down list.

Step 16 Click **Submit**.

Troubleshooting

UCS Director Fails with Flex Error 1001: Digest Mismatch with RSL

Problem—After a Cisco UCS Director upgrade, access to the GUI sometimes fails with the following error, immediately after logging in:

```
Flex Error #1001: Digest mismatch with RSL
    http://10.5.40.10/app/cloudmgr/cloupia_common.swf. Redeploy the matching RSL or
    relink your application with the matching library.
```

Possible Cause—This can happen after an upgrade of the Cisco UCS Director appliance. Exact conditions are not known at this time.

Recommended Solution— Cisco recommends the following workarounds:

Step 1 Clear the browser cache.

Step 2 Restart the browser (or all open browsers).

Step 3 Use a different browser.

Step 4 Perform a browser reset, as described in the following documents. This will erase any previously configured browser settings.

- For Firefox, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.
- For Internet Explorer, see http://windows.microsoft.com/en-us/internet-explorer/reset-ie-settings#ie=ie-11.

UCS Director Upgrade Does Not Respond

Problem—When applying a patch upgrade to the nodes of a Cisco UCS Director single-node or multi-node deployment, the upgrade does not respond.

Possible Cause—This can occur if the time on the nodes is not synchronized.

Recommended Solution—Resync the NTP time and time zone information on each node:

SUMMARY STEPS

1. Stop the upgrade in process.
2. Manually resync the NTP server settings using the **Time Sync** shell admin option in the standalone (single-node) and primary, service, inventory, and monitoring nodes.
3. Restart the upgrade process.

DETAILED STEPS

Step 1 Stop the upgrade in process.

Step 2 Manually resync the NTP server settings using the **Time Sync** shell admin option in the standalone (single-node) and primary, service, inventory, and monitoring nodes.

Step 3 Restart the upgrade process.

© 2016 Cisco Systems, Inc. All rights reserved.